UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/895,788	06/29/2001	Thomas L. Stachura	42390P10773	5580

8791 7590 11/02/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 11/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/895,788	STACHURA ET AL.	
	Examiner	Art Unit	
	Eleni A Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 are presented for examination.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1,3-4, 20-23, and 25-30 are rejected under 35 U.S.C. 102(b) as being anticipated by Skret (US Patent Number: 5,001,755).

As per claim 1 Skret teaches a method comprising:

establishing secured communication between a client device and server device (Skret Col. 2 lines 57-col. 3 lines 11);

wherein communication is secured using, at least in part, synchronized security sequence value(s) (Skret Col. 2 lines 10-27, col. 11 lines 60-68, Fig. 3A No. 112; Sequence number field for carrying sequence value);

storing a security sequence value as a resynchronization value (Skret Col. 5 lines 41-col. 6 lines 2; sequence counts are stored in RAM);

detecting at least one event desynchronizing said secured communication (Skret Col. 2 lines 10-27); and

requesting resynchronization of security sequence values (Skret Col. 6 liens 7-17; sending a message to the transmitting node indicating that it is out of synchronization and requesting resynchronization), comprising sending at least a representation of said resynchronization value from said client device to said server device (Skret Col. 6 lines 7-lines 26, Fig. 3A No. 112; Sequence number field for carrying sequence value).

As per claim 20, Skret teaches a method comprising:

establishing secured communication between a security interface and a network node (Skret Col. 2 lines 10-27; receiving node is synchronized with the transmitting node), said security interface to resynchronize security sequence values between said security interface and said network node (Skret Col. 2 lines 10-27; a mechanism for resynchronizing two nodes);

storing a first resynchronization value selected by said security interface (Skret Col. 5 lines 42-col. 6 lines 2; sequence counts are stored in RAM); and

resynchronizing said security sequence values after a break in said secured communication (Skret Col. 2 lines 10-27; resynchronizing mechanism is provided to resynchronize when synchronization is lost due to the loss of power or other reason), said resynchronizing further comprising:

sending said first resynchronization value from said security interface to said network node (Skret Col. 6 lines 18-26; transmitting resynchronization key between two nodes);

sending said first resynchronization value and a second resynchronization value from said network node to said security interface (Skret Col. 6 lines 18-26; transmitting resynchronization key between two nodes, and new transmitting key may vary from the starting key); and

reestablishing said secured communication using said first resynchronization value and said second resynchronization value (Skret Col. 2 lines 10-27 reestablishing mechanism to establish secure communication between two devices when synchronization is lost due to power).

As per claim 28, Skret teaches a method, comprising:

establishing secured communication between a server device and a client device (Skret Col. 5 lines 42-col. 6 lines 2; two devices are simultaneously initiate communication with each other), said secured communication using server security sequence values synchronized with client security sequence values (Skret Col. 7 lines 1-7);

storing at least one client security sequence value in nonvolatile memory as a saved client security sequence value (Skret Col. 6 lines 42-col. 7 lines 2; sequence counts are stored in RAM); and

resynchronizing server and client security sequence values after a desynchronization event by sending said saved client security sequence value from said nonvolatile memory to said server device (Skret Col. 2 lines 10-27 reestablishing mechanism to establish secure communication between two devices when synchronization is lost due to power).

As per claim 3, Skret teaches a method, wherein sending at least a representation of said resynchronization value includes embedding said resynchronization value in at least one header and/or at least one payload of a data packet (Skret Fig. 3A-3D).

As per claim 4, Skret teaches a method, wherein said storing a client resynchronization value includes periodically refreshing a stored value with a new value at a selected interval from security sequence values already used in a secured communication session (Skret Col. 4 lines 48-59).

As per claim 21, Skret teaches a method further comprising using a security interface as a state machine in network circuitry (Skret Col. 1 lines 11-24).

As per claim 22, Skret teaches a method further comprising using a security interface as a software program (Skret Col. 5 lines 42-67).

As per claim 23, Skret teaches a method further comprising storing said first resynchronization value in a nonvolatile storage medium (Skret Col. 6 lines 1-2).

As per claim 25, Skret teaches a method further comprising resynchronizing said secured communication using said first resynchronization value to resynchronize secured data sent from said security interface and using said second resynchronization value to resynchronize secured data sent from said network node (Skret Col. 2 lines 10-27, and col. 6 lines 18-26).

As per claim 26, Skret teaches a method further comprising resynchronizing secured communication during a low-power state (Skret Col. 2 lines 10-27).

As per claim 27, Skret teaches a method further comprising resynchronizing secured communication while said network node lacks an active operating system and/or lacks an active microprocessor (Skret Col. 2 lines 10-27; loss of power or other reasons).

As per claim 29, Skret teaches a method, said resynchronizing further comprising returning said saved client security sequence value from said server device to said client device in a data packet with a server security sequence value (Skret Col. 2 lines 10-27, and Fig. 3A no. 116).

As per claim 30, Skret teaches a method said storing further comprising periodically refreshing said saved client security sequence value with a number that is greater in value than client security sequence values that have already been sent to said server device in a communication session (Skret Col 4 lines 48-59, and Col. 6 lines 18-26).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 5-9, and 11-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Skret (US Patent Number: 5,001,755) in view of Trachewsky et al. (Trachewsky, Pub. No.: US 2003/0206559 A1).

As per claim 5 Skret teaches a method comprising:

establishing secured communication between a client device and server device (Skret Col. 2 lines 57-col. 3 lines 11);

wherein communication is secured using, at least in part, synchronized security sequence value(s) (Skret Col. 2 lines 10-27, col. 11 lines 60-68);

sending at least a representation of said request for resynchronization and a server resynchronization value from said server device to said client device (Skret Col. 6 lines 7-lines 26, Fig. 3A); and

reestablishing secured communication using said server resynchronization value (Skret Col. 2 lines 10-27 reestablishing mechanism to establish secure communication between two devices when synchronization is lost due to power);

Skret does not explicitly teach acknowledging a client request for resynchronization,

However Trachewsky discloses acknowledging a client request in using sequence value (Trachewsky Page 60 par. 0458);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Trachewsky with in the system of Skret because it would allow to verify the acknowledgment of a sequence to other nodes (Trachewsky Page 59 par. 0454) Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to acknowledge a client request for resynchronization

because it would verify a client that the communication is resynchronized securely after desynchronization event occur when power loss.

As per claim 14, Skret teaches an apparatus, comprising;

(a) a security interface to engage in secured communication with at least one network node, wherein said security interface and said at least one network node use synchronized security sequence values at least in part to authenticate said secured communication (Skret Col. 2 lines 10-25);

(i) a recorder to store at least one security sequence value (Skret Col. 5 lines 42-col. 6 lines 2; sequence counts are stored in RAM);

(ii) a desynchronization detector coupled to said security interface (Skret Col. 2 lines 10-27; desynchronization is detected due to the loss of power);

(iii) a resynchronization requester to send the stored security sequence value to at least one network node after a desynchronization (Skret Col. 6 lines 7-lines 26; resynchronization request transmitted over a secure network between two devices); and

(b) a security agent coupled to said at least one network node (Skret Col. 1 lines 41-51; data communication network techniques to a security system), comprising:

(i) a request receiver to recognize said stored security sequence value (Skret Col. 6 lines 18-27; request for resynchronization is received);

Skret does not explicitly teach verifier to receive feedback from said at least one network node;

(ii) an acknowledger to send said feedback from said security agent to said security interface; said feedback comprising said stored security sequence value and a node security sequence value from said network node.

However Trachewsky discloses acknowledging a client request in using sequence value that reads on verifying to receive feedback from said at least one network node (Trachewsky Page 60 par. 458);

(ii) an acknowledger to send said feedback from said security agent to said security interface; said feedback comprising said stored security sequence value and a node security sequence value from said network node (Trachewsky Page 60 par. 458);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Trachewsky with in the system of Skret because it would allow to verify the acknowledgment of a sequence to other nodes (Trachewsky Page 59 par. 0454) Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to acknowledge a client request for resynchronization because it would verify a client that the communication is resynchronized securely after desynchronization event occur when power loss.

As per claim 17, Skret teaches a computer network security sequence value resynchronizer, comprising:

(a) a sender having at least access to a nonvolatile random access memory (Skret Col. 4 lines 47-59);

(b) said sender to transmit a data packet containing at least in part a stored sender resynchronization value from said nonvolatile random access memory over said computer network (Skret Fig. 3A, and Col. 9 lines 21-43);

computer network to receive said sender resynchronization value from said sender (Skret Col. 13 lines 57-60); and returning said sender resynchronization value to said sender as security assurance (Skret Col. 13 lines 57-60);

Skret does not explicitly teach (c) an acknowledger connected to said computer network to receive said sender resynchronization value from said sender (Trachewsky Page 60 par. 458); said acknowledger returning said sender resynchronization value to said sender as security assurance (Trachewsky Page 60 par. 458);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Trachewsky with in the system of Skret because it would allow to verify the acknowledgment of a sequence to other nodes (Trachewsky Page 59 par. 0454) Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to acknowledge a client request for resynchronization because it would verify a client that the communication is resynchronized securely after desynchronization event occur when power loss.

As per claim 6, Skret teaches a method, wherein said client request for resynchronization is a client resynchronization value and said secured communication is reestablished using said client resynchronization value and said server resynchronization value (Skret Col. 2 lines 10-27 reestablishing mechanism to establish secure communication between two devices when synchronization is lost due to power).

As per claim 7, Skret and Trachewsky teach all the subject matter as described above. In addition Skret teaches a method, wherein sending at least a representation of said client and said server resynchronization values includes embedding said client and said server resynchronization values in at least one header and/or at least one payload of a data packet that conforms to IPsec standards (Skret Fig. 3A-3D).

As per claim 8, Skret and Trachewsky teach all the subject matter as described above. In addition Skret teaches a method, further comprising performing said method using a state machine in network circuitry (Skret Col. 1 lines 11-24).

As per claim 9, Skret and Trachewsky teach all the subject matter as described above. In addition Skret teaches a method, further comprising using software to perform said method (Skret Col. 5 lines 42-67).

As per claim 11, Skret and Trachewsky teach all the subject matter as described above. In addition Skret teaches a method, further comprising reestablishing secured communication

during a low-power state (Skret Col. 2 lines 10-27).

As per claim 12, Skret and Trachewsky teach all the subject matter as described above. In addition Skret teaches a method, further comprising reestablishing secured communication while said first device lacks an active operating system and/or lacks an active microprocessor (Skret Col. 2 lines 10-27; loss of power or other reasons).

As per claim 13, Skret and Trachewsky teach all the subject matter as described above. In addition Skret teaches a method, further comprising a machine-readable medium that provides instructions, which when executed by at least one electronic circuit, cause said at least one electronic circuit to perform operations comprising said method (Skret Col. 4 lines 47-59).

As per claim 15, Skret and Trachewsky teach all the subject matter as described above. In addition Skret teaches the apparatus, wherein stored security sequence values and node security sequence values are embedded in at least one header and/or at least one payload of a data packet that conforms to IPsec standards (Skret Fig. 3A-3D).

As per claim 16, Skret and Trachewsky teach all the subject matter as described above. In addition Skret teaches the apparatus, wherein said stored security sequence value is periodically refreshed with a value at a selected interval from security sequence values already used in a secured communication session (Skret Col. 4 lines 48-59).

As per claim 18, Skret and Trachewsky teach all the subject matter as described above. In addition Trachewsky teaches the resynchronizer, said acknowledger returning an acknowledger resynchronization value to said sender in addition to said sender resynchronization value (Trachewsky Page 60 par. 0458). The rational for combining are the same as claim 17 above.

As per claim 19, Skret and Trachewsky teach all the subject matter as described above. In addition Trachewsky teaches the resynchronizer, wherein at least one sender and at least one acknowledger are installed on any combination of server and client devices (Trachewsky Page. 59 par. 0453; a client node requests a sequence value and a master node acknowledges using sequence value).

6. Claims 2, 10, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Skret (US Patent Number: 5,001,755) in view of Trachewsky et al. (Trachewsky, Pub. No.: US 2003/0206559 A1), and in further view of Dixon et al. (Dixon, US Patent No. 6,697,857 B1).

As per claim 2 and 10, Skret and Trachewsky teach all the subject matter as described above.

Skret and Trachewsky do not explicitly teach performing anti-replay filtering;

However Dixon teaches a method, further comprising performing anti-replay filtering using said security sequence values (Dixon Col. 1 lines 28-41);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Dixon with in the combination system of Skret and Trachewsky because it would allow to operate at the network layer to secure most

types of IP packets (Dixon Col. 1 lines 28-40); Therefore it would have been obvious to one having ordinary skilled in the art at the time of the invention was made to apply the teachings of Dixon because it would ignore the data packets that have been previously received.

As per claim 24, Skret and Trachewsky teach all the subject matter as described above.

Skret and Trachewsky do not explicitly teach IPsec,

However Dixon discloses a method further comprising establishing secured communication using IPsec security standards (Dixon Col. 1 lines 27-41).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Dixon with in the combination system of Skret and Trachewsky because it would allow to operate at the network layer to secure most types of IP packets, and the authentication header would provide data communication with source authentication and integrity, while the encapsulated security payload provides confidentiality as well as a limited degree of source authentication (Dixon Col. 1 lines 28-40); Therefore it would have been obvious to one having ordinary skilled in the art at the time of the invention was made to apply the teachings of Dixon because it would authenticate the integrity of data transmitted between two nodes.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 703-305-0326. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
Art Unit 2136

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100